

What is claimed is:

1. A digital certificate, comprising:
a distinguished name (DN) field; and
a common name (CN) field within the DN field, containing a resource identifier,
wherein the resource identifier contains information identifying each of a plurality of
certificate-issuing resources in the certification path of the digital certificate.
2. The digital certificate of claim 1, wherein the resource identifier is a
hierarchical identifier specifying an identity of a trusted root resource, and an identity of a
resource issuing the digital certificate.
3. The digital certificate of claim 1, wherein the resource identifier further
contains identifiers of certificate-issuing resources in a certification path between the trusted
root resource and the resource issuing the digital certificate.
4. The digital certificate of claim 1, wherein the digital certificate is for use in a
computing system, and the certification path leads to a trusted source for the computing
system.
5. A method for generating a digital certificate with an authority identification
field, comprising:
signing the digital certificate; and
inserting into the authority identification field a resource identifier that contains
information identifying each of a plurality of certificate-issuing resources in a certification
path of the digital certificate.
6. The method of claim 5, wherein the resource identifier is a hierarchical
identifier specifying an identity of a trusted root resource, and an identity of a resource
issuing the digital certificate.

7. The method of claim 5, wherein the resource identifier further contains identifiers of resources in a certification path between the trusted root resource and the resource issuing the digital certificate.

8. The method of claim 5, wherein the digital certificate is for use in a computing system, and the certification path leads to a trusted source for the computing system.

9. A computer readable medium of program instructions for generating a digital certificate with an authority identification field, the program instructions executable by a computer to perform a method comprising:

signing the digital certificate; and

inserting into the authority identification field a resource identifier that contains information identifying each of a plurality of certificate-issuing resources in a certification path of the digital certificate.

10. The computer readable medium of claim 9, wherein the resource identifier is a hierarchical identifier specifying an identity of a trusted root resource, and an identity of a resource issuing the digital certificate.

11. The computer readable medium of claim 9, wherein the resource identifier further contains identifiers of resources in a certification path between the trusted root resource and the resource issuing the digital certificate.

12. The computer readable medium of claim 9, wherein the digital certificate is for use in a computing system, and the certification path leads to a trusted source for the computing system.

13. A method of revoking a digital certificate having an authority identification field containing a resource identifier that contains information identifying each of a plurality of certificate-issuing resources in a certification path of the digital certificate, the method comprising:

identifying the certificate-issuing resource that issued the digital certificate based on the resource identifier in the authority identification field of the digital certificate; and

querying the certificate-issuing resource to determine if the digital certificate has been revoked.

14. The method of claim 13, wherein the resource identifier is a hierarchical identifier specifying an identity of a trusted root resource and an identity of the certificate-issuing resource.

15. The method of claim 13, wherein the resource identifier further contains identifiers of resources in a certification path between the trusted root resource and the certificate-issuing resource.

16. The method of claim 13, wherein the digital certificate is for use in a computing system, and the certification path leads to a trusted source for the computing system.